Научная статья
УДК 004.056+003.26
https://doi.org/10.24143/2072-9502-2026-2-53-60
EDN IUAEIH

Модификация постквантового механизма инкапсуляции ключей «Земляника»

Надежда Валерьевна Давидюк✉, Феликс Загидинович Эфендиев, Георгий Александрович Попов

Астраханский государственный технический университет,
Астрахань, Россия, n.davidyuk@astu.ru✉

Аннотация. Криптографическая схема механизма инкапсуляции ключей (Key Encapsulation Mechanism, KEM) Zemlyanika («Земляника»), основанная на проблеме модульного обучения с ошибками (Module-Learning With Errors, Module-LWE), использует модуль редукции в форме степени двойки, что обеспечивает высокоэффективную модульную арифметику, но исключает применение теоретико-числового преобразования (Number Theoretic Transform, NTT) для осуществления полиномиального умножения. Это приводит к использованию асимптотически менее эффективных и приближенных алгоритмов, вызывающих проблемы с точностью, гибкостью параметризации и сложностью защиты от атак по побочным каналам. Целью исследования является преодоление системных ограничений оригинальной схемы за счет замены модуля редукции на квазистепенной. Научная новизна заключается в комплексном анализе корректности и стойкости модифицированной схемы при таком переходе. Показано, что предлагаемый модуль редукции позволяет реализовать асимптотически оптимальное NTT-умножение, сохранив при этом эффективную редукцию, близкую по скорости к редукции с применением степенного модуля. Условие корректности декапсуляции ужесточается незначительно (снижение границы корректности примерно на 0,49 %), что является контролируемым и компенсируемым. Показано, что использование простого модуля редукции аналогичного размера не оказывает существенного влияния на сложность известных решеточных атак в модели Core-SVP, поскольку стойкость определяется геометрическими свойствами решетки, а не арифметикой модуля редукции. Результатом работы является сбалансированное архитектурное решение, повышающее вычислительную эффективность и гибкость параметризации KEM Zemlyanika без ущерба для криптографической стойкости, с прогнозируемым ускорением операций инкапсуляции и декапсуляции в 1,8–2,6 раза для различных наборов параметров.

Ключевые слова: KEM Zemlyanika, постквантовая криптография, Module-LWE, NTT, квазистепенной модуль, полиномиальное умножение, криптографическая стойкость, корректность схемы

Для цитирования: *Давидюк Н. В., Эфендиев Ф. З., Попов Г. А.* Модификация постквантового механизма инкапсуляции ключей «Земляника» // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2026. № 2. С. 53–60. https://doi.org/10.24143/2072-9502-2026-2-53-60. EDN IUAEIH.

Original article

Modification of the post-quantum key encapsulation mechanism “Zemlyanika”

Nadezhda V. Davidyuk✉, Felix Z. Efendiev, Georgy A. Popov

Astrakhan State Technical University,
Astrakhan, Russia, n.davidyuk@astu.ru✉

Abstract. The cryptographic scheme of the key encapsulation mechanism (KEM) Zemlyanika (“Strawberry”), based on the problem of modular learning with errors (Module-Learning With Errors, Module-LWE), uses a reduction module in the form of a power of two, which provides highly efficient modular arithmetic, but excludes the use of number-theoretic transformations (Number Theoretical Transform, NTT) for performing polynomial multiplication. This leads to the use of asymptotically less efficient and approximate algorithms, which cause problems with accuracy, flexibility

of parameterization, and complexity of protection against side-channel attacks. The purpose of the study is to overcome the system limitations of the original scheme by replacing the reduction module with a quasi-secondary one. The scientific novelty lies in a comprehensive analysis of the correctness and stability of the modified scheme during such a transition. It is shown that the proposed reduction module makes it possible to implement asymptotically optimal NTT multiplication, while maintaining an effective reduction that is close in speed to power-law reduction. The decapsulation correctness condition is slightly tightened (a decrease in the correctness limit by about 0.49%), which is controllable and compensable. It is shown that the use of a simple reduction module of a similar size does not significantly affect the complexity of known lattice attacks in the Core-SVP model, since durability is determined by the geometric properties of the lattice, rather than the arithmetic of the reduction module. The result of the work is a balanced architectural solution that increases the computational efficiency and flexibility of KEM Zemlyanika parameterization without compromising cryptographic strength, with a predicted acceleration of encapsulation and decapsulation operations by 1.8-2.6 times for various parameter sets.

Keywords: KEM Zemlyanika, post-quantum cryptography, Module-LWE, NTT, quasi-power-of-two modulus, polynomial multiplication, cryptographic security, scheme correctness

For citation: Davidyuk N. V., Efendiev F. Z., Popov G. A. Modification of the post-quantum key encapsulation mechanism “Zemlyanika”. *Vestnik of Astrakhan State Technical University. Series: Management, computer science and informatics*. 2026;2:53-60. (In Russ.). https://doi.org/10.24143/2072-9502-2026-2-53-60. EDN IUAEIH.

Введение

На протяжении всей истории развития криптографии обеспечение конфиденциальности и подлинности информации являлось одной из первостепенных задач. Прогнозируемое в ближайшие два десятилетия появление квантовых компьютеров создало новые вызовы, поскольку традиционные криптографические системы оказались потенциально незащищенными. Это обстоятельство стимулировало активное развитие постквантовой криптографии, ориентированной на создание алгоритмов, устойчивых к атакам как классического, так и квантового компьютера.

Постквантовая криптография приобретает особую значимость в условиях роста угроз, связанных с развитием квантовых вычислений, которые способны подорвать безопасность существующих систем защиты данных – как на этапах обработки и хранения данных, так и при их передаче. Для обеспечения конкурентоспособности и государственного суверенитета в области цифровой безопасности необходимы отечественные криптографические алгоритмы с высокой производительностью, допускающие эффективную интеграцию в существующие информационные инфраструктуры. Разработки в данной сфере играют важную роль в этом процессе, однако требуют дальнейшей оптимизации для достижения баланса между вычислительной эффективностью и криптографической стойкостью. В условиях глобальной конкуренции повышение производительности постквантовых схем способствует укреплению технологической независимости Российской Федерации. Отметим, что под инкапсуляцией ключей понимается криптосистема с открытым ключом, которая позволяет отправителю генерировать короткий секретный ключ и передавать его получателю конфиденциально, несмотря на подслушивание и перехват злоумышленниками. Эта процедура особенно актуальна для процесса передачи данных по квантовым каналам [1].

Среди множества подходов к разработке постквантовых криптографических механизмов особое внимание привлекают схемы, основанные на задачах обучения с ошибками (Learning With Errors, LWE) и их модульных обобщениях (т. е. в модульной арифметике (M-LWE) [1–3], к числу которых относится механизм инкапсуляции ключей KEM Zemlyanika (Key Encapsulation Mechanism, KEM «Земляника») [4]. Данные конструкции демонстрируют благоприятный компромисс между эффективностью реализации и криптографической надежностью, что подтверждается их выбором в качестве основы для современных стандартов постквантовой криптографии. Отметим, что в целом механизмы инкапсуляции ключей представляют собой функциональные аналоги, например, протокола Диффи – Хеллмана, но в KEM ключ не создается совместно участниками, а генерируется одной стороной, шифруется и передается второй. Для выработки ключа в KEM используются алгоритмы шифрования с открытым ключом. Механизм инкапсуляции ключей включает три алгоритма [1]:

– генерации ключа (KeyGen) – генерирует ключевую пару (открытый и закрытый ключи);

– инкапсуляции (Encaps) – принимает открытый ключ, случайным образом выбирает секретный ключ и возвращает его вместе с инкапсуляцией;

– декапсуляции (Decaps) – принимает закрытый ключ и инкапсуляцию и либо возвращает инкапсулированный секретный ключ, либо завершается ошибкой.

В настоящее время известны различные алгоритмы постквантовой криптографии [4–6], в частности ML-KEM (Kyber) – механизм инкапсуляции ключей на основе модульных решеток, ML-DSA (Dilithium) – алгоритм цифровой подписи на основе модульных решеток (FIPS-204), SLH-DSA (SPHINCS+) – алгоритм цифровой подписи на ос-

нове хеш-функций, исследуемый в работе KEM Zemlyanika. При этом продолжаются исследования, направленные на разработку новых и усовершенствование существующих схем на основе модульного обучения с ошибками (Module-Learning With Errors, Module-LWE) с целью повышения скорости их работы, уменьшения размеров ключей и шифротекстов, а также повышения устойчивости к различным видам атак. Существенную роль в проектировании таких схем играет выбор математических параметров, в частности модуля редукции (т. е. основания операций модульной арифметики), который непосредственно влияет как на быстродействие, так и на устойчивость всей криптографической схемы.

Целью настоящего исследования является анализ архитектурных решений механизмов инкапсуляции ключей на основе Module-LWE и разработка подхода к модификации KEM Zemlyanika, направленной на повышение вычислительной эффективности при сохранении криптографической стойкости.

Для достижения поставленной цели в работе решаются следующие задачи:

1. Проведение анализа архитектурных и алгоритмических особенностей оригинальной схемы KEM Zemlyanika.

2. Исследование влияния выбора модуля редукции на корректность, криптографическую стойкость и вычислительную эффективность модифицированной схемы KEM.

3. Оценка прогнозируемого выигрыша в производительности операций инкапсуляции и декапсуляции при использовании теоретико-числового преобразования (Number Theoretic Transform, NTT).

В рамках данного исследования предлагается переход к использованию квазистепенного модуля редукции в постквантовой схеме инкапсуляции ключей KEM Zemlyanika, что позволяет интегрировать теоретико-числовое преобразование NTT для реализации полиномиального умножения.

Анализ архитектурных решений и алгоритмических особенностей KEM Zemlyanika

Криптографическая схема механизма инкапсуляции ключей KEM Zemlyanika [4] является перспективной разработкой на основе Module-LWE (M-LWE), характеризующейся использованием модуля редукции специальной структуры и явным выраженным механизмом отклонения. Одним из ключевых аспектов KEM Zemlyanika является применение модуля редукции в форме степени двойки. Такой выбор позволяет реализовать высокоэффективную модульную арифметику, основанную на побитовых операциях, что благоприятно сказывается на быстродействии операций генерации матриц и редукции. Однако данный подход влечет за собой ряд ограничений, затрагивающих как производительность, так и архитектурную гибкость схемы.

Главным следствием выбора модуля редукции в виде степени двойки является невозможность использования теоретико-числового преобразования (NTT) [5] – наиболее эффективного метода полиномиального умножения в схемах, основанных на решетках [1, 7]. В результате в KEM Zemlyanika применяется комбинация алгоритмов Toom-Cook [8], Karatsuba [4] и классического алгоритма умножения. Несмотря на приемлемую практическую производительность, данные методы как асимптотически, так и на практике уступают NTT, что приводит к увеличению вычислительных затрат при практической реализации [8].

Как отмечают авторы схемы KEM Zemlyanika, использование степенного модуля предоставляет ряд преимуществ, которые часто недооцениваются [4]. К таким преимуществам относится высокая эффективность генерации случайных матриц и выполнения модульной редукции, реализуемой с использованием простых алгоритмов, таких как редукции Монтгомери или Барретта [9]. Подобные алгоритмы оптимизации демонстрируют существенный выигрыш в производительности: например, в работе [10] показано, что сокращение числа модульных редукций в схеме Kyber позволило ускорить алгоритмы на 40–80 %. Таким образом, выбор степенного модуля в KEM Zemlyanika изначально был обоснован стремлением к максимальной эффективности на уровне элементарных операций.

Однако за указанные преимущества приходится платить на уровне полиномиальной арифметики. Поскольку применение NTT требует существования примитивного корня степени $2n$ в поле, его использование для модуля вида

$$q = 2^t \tag{1}$$

является невозможным, что представляет собой фундаментальное алгебраическое ограничение.

В результате разработчикам KEM Zemlyanika пришлось реализовать высокооптимизированную комбинацию методов Toom-4, Karatsuba и алгоритма schoolbook-умножения. В частности, для наборов параметров Z512 и Z768-R используется алгоритм Toom-4-4, эквивалентный по вычислительным затратам 49 умножениям полиномов степени 15 с использованием классического алгоритма.

Существенным недостатком алгоритмов семейства Toom-Cook является потеря точности. В отличие от достаточно точного NTT данные методы являются приближенными: каждый этап декомпозиции приводит к уменьшению точности представления коэффициентов. Так, применяемый в KEM Zemlyanika алгоритм Toom-4-4 приводит к потере до 6 бит точности. В сочетании со степенным мо-

дулем это вызывает две взаимосвязанные проблемы: необходимость увеличения разрядности промежуточных переменных и ограничения при выборе параметров схемы. Как указано в [4], для параметров Z768-C и Z1024 использование Toom-4-4 оказалось невозможным из-за чрезмерной потери точности, что потребовало перехода к менее эффективному гибридному алгоритму Toom-4-2-2. Таким образом, потеря точности напрямую влияет на гибкость и оптимальность параметризации схемы.

Кроме того, сложные нелинейные и приближенные алгоритмы умножения создают риски на уровне практической реализации. Их высокая структурная сложность затрудняет защиту от атак по побочным каналам и усложняет формальную верификацию корректности реализации. Накопление ошибок округления требует проведения дополнительного анализа для гарантии того, что итоговая ошибка не приведет к увеличению вероятности криптографического сбоя.

Таким образом, анализ оригинальной схемы KEM Zemlyanika выявляет фундаментальный архитектурный компромисс: максимальная эффективность модульной арифметики достигается ценой снижения эффективности полиномиального умножения. Это создает естественную предпосылку для поиска решения, которое сохранило бы преимущества степенного модуля редукции и одновременно обеспечило возможность использования высокоскоростного и точного NTT-умножения.

Подход к модификации KEM Zemlyanika за счет изменения модуля редукции

Выявленные ограничения схемы KEM Zemlyanika связаны с выбором модуля редукции в форме степени двойки, который, обеспечивая высокую эффективность модульной арифметики, одновременно исключает возможность применения NTT для полиномиального умножения. Для устранения данного противоречия требуется модуль редукции, сохраняющий вычислительные преимущества степени двойки и обладающий алгебраическими свойствами, необходимыми для использования NTT.

В качестве такого решения предлагается переход к квазистепенному модулю редукции вида

$$q = 2^t - \delta, \tag{2}$$

где δ – положительное целое число, подобранное таким образом, чтобы q являлось простым числом. Данный выбор представляет собой не просто модификацию параметра, а качественное изменение архитектурного фундамента схемы, позволяющее синтезировать ранее несовместимые преимущества.

Переход от степенного модуля (1) к квазистепенному (2) не приводит к изменению общей структуры KEM Zemlyanika, однако оказывает существенное влияние на реализацию ключевых вычислительных этапов. Ключевым достоинством квазистепенного модуля редукции (2) является возможность реализации высокоэффективного алгоритма модульной редукции, по быстродействию близкого к редукции по модулю степени двойки (1). Для значения $x < q^2$ редукция по квазистепенному модулю может быть выполнена с использованием простой последовательности операций, основанной на разложении числа на старшие и младшие биты. В частности, вычисляются младшие t бит числа x, старшая часть получается с помощью логического сдвига вправо, после чего итоговое значение формируется путем сложения младшей части с произведением старшей части на параметр δ.

Данный метод, по сути, является адаптацией алгоритма Барретта с константной вычислительной сложностью O (1), который может быть реализован с использованием лишь сложения, битовых сдвигов и однократного умножения на малую константу δ, что делает его крайне эффективным для вычислений на современных процессорах. Таким образом, сохраняется одно из главных преимуществ степенного модуля – скорость модульной редукции, что критически важно для операций генерации матриц и векторных операций, характерных для M-LWE.

Наиболее значительное архитектурное преимущество квазистепенного модуля – это возможность сделать его простым числом, удовлетворяющим алгебраическому условию

$$q \equiv 1 (\mathrm{mod}\ 2n). \tag{3}$$

Это условие является необходимым и достаточным для существования в поле $\mathbb{Z}_q$ примитивного корня степени $2n$, что, в свою очередь, позволяет определить и вычислить NTT.

NTT является аналогом быстрого преобразования Фурье в конечных полях и позволяет выполнять умножение полиномов в кольце:

$$R_q = \mathbb{Z}_q[x] / (x^n + 1) \tag{4}$$

за время $O(n \log n)$, что асимптотически и практически значительно быстрее комбинации Toom-Cook и Karatsuba, используемых в Zemlyanika, которые имеют сложность порядка $O(n^{1,46})\ldots O(n^{1,58})$ и требуют трудоемкой реализации с потерей точности.

Использование NTT является стандартной и отлаженной практикой в таких схемах инкапсуляции ключей, как Kyber [11] и Dilithium [6]. Его применение не только ускоряет шифрование и расшифрование, но и вносит следующие улучшения:

– скорость алгоритмов Encaps и Decaps значительно увеличивается, т. к. полиномиальное умножение является их вычислительным ядром;

– линейная и регулярная структура NTT-преобразования проще для анализа и формальной верификации по сравнению с нелинейными и многостадийными алгоритмами;

– в отличие от приближенных методов NTT является точным алгоритмом в конечном поле, что исключает необходимость анализа накопления ошибок и использования буферных битов, упрощая управление памятью.

Для наглядной демонстрации преимуществ предлагаемого подхода к модификации Zemlyanika на основе доступных данных и вычислительных экспериментов был проведен сравнительный анализ ключевых характеристик для трех типов модулей, результаты которого приведены в табл. 1.

Таблица 1

Table 1

Сравнительный анализ характеристик модулей для KEM на основе M-LWE

Comparative analysis of the characteristics of modules for KEM based on M-LWE

Критерий	**Вид модуля**		
	$q = 2^t$	$q = 256k + 1$	$q = 2^t - \delta$
Возможность применить NTT	Нет	Да	
Скорость полиномиального умножения	$O(n^{1,46})$	$O(n \log n)$	
Скорость модульной редукции	Максимальная (побитовая операция)	Средняя (алгоритмы Барретта и Монтгомери)	Очень высокая
Требования к памяти	Минимальные	Стандартные	Минимальные
Гибкость и параметризации	Ограничена	Высокая	
Стойкость к атакам на M-LWE	Высокая	Средняя	
Удобство защиты от побочных каналов	Сложное	Стандартное	

Сравнительный анализ модулей показывает, что квазистепенной модуль занимает промежуточное, но выигрышное положение: он сочетает возможность применения NTT и высокую скорость модульной редукции, при этом сохраняет минимальные требования к памяти и гибкость параметризации, сравнимую с другими современными постквантовыми схемами инкапсуляции ключей.

Переход на квазистепенной модуль (2) требует строгой проверки двух фундаментальных аспектов: сохранения корректности работы алгоритмов и обеспечения криптографической стойкости на уровне исходной схемы.

Условие корректного расшифрования в схеме Zemlyanika имеет вид

$$\| e^T r - S^T \left(e_1\, e_u\right) e_2\, e_v \|_\infty < \frac{q}{4}.$$

При переходе на новый модуль (2) правая часть выражения (4) уменьшается пропорционально уменьшению модуля:

$$\frac{q'}{4} = \frac{2^t - \delta}{4} < \frac{2^t}{4},$$

что формально ужесточает условие корректности. Параметр при переходе на границе корректности уменьшается с 256 до 254,75, т. е. примерно на 0,49 %. Тем не менее, как показывает анализ, данное увеличение вероятности сбоя является предсказуемым и контролируемым. Незначительность изменений позволяет эффективно компенсировать их за счет минимальной корректировки параметров шума либо использования модуля с незначительно увеличенной разрядностью. Криптографическая стойкость схемы при этом сохраняется, поскольку сложность задачи Module-LWE определяется геометрическими свойствами решетки, а не арифметикой модуля. Сохранение битовой длины q и дисперсий шума обеспечивает уровень безопасности, сопоставимый с исходной схемой, а применение NTT не добавляет новых рисков, т. к. это вычислительная техника, не изменяющая математическую структуру задачи.

Таким образом, предлагаемая в работе модификация KEM Zemlyanika обеспечивает предсказуемую корректность работы, сохраняет криптографическую стойкость и дает системный выигрыш в производительности благодаря оптимизации полиномиального умножения через NTT при сохранении высокой скорости модульной арифметики. Переход на квазистепенной модуль (2) представляет собой сбалансированное решение, которое устраняет ключевые архитектурные ограничения оригинальной схемы, повышая эффективность вычислений и одновременно сохраняя криптографическую надежность, создавая основу для более технологичной реализации KEM на базе M-LWE.

Апробация предлагаемого архитектурного решения

Переход на квазистепенной модуль в схеме KEM Zemlyanika, как было показано в предыдущих разде-

лах, теоретически позволяет сохранить криптографическую стойкость и корректность работы, одновременно открывая возможность применения высокоэффективного NTT-умножения. Для количественной оценки практического эффекта данной модификации была проведена апробация, основанная на аналитической модели производительности в рамках классического алгоритма инкапсуляции [1–4]. В основе модели лежит декомпозиция процедуры выполнения алгоритмов на составляющие, где доминирующую роль играют операции полиномиального умножения, количество которых квадратично зависит от размерности модуля k. На основе оценки ускорения за счет применения NTT и данных эталонной реализации модель позволяет спрогнозировать итоговое ускорение для ключевых операций схемы.

Результаты, демонстрирующие количественный выигрыш в производительности для двух основных параметризаций KEM Zemlyanika Z512 и Z1024, представлены в табл. 2.

Таблица 2

Table 2

Сравнительный анализ производительности оригинальной и модифицированной схем KEM Zemlyanika

Comparative performance analysis of the original and modified KEM Zemlyanika circuits

Набор параметров	Алгоритм	Оригинальное время, мкс	Прогнозируемое время с NTT, мкс	Прогнозируемое ускорение, разы
Z512	KeyGen	11,5	~10,3	~1,12
	Encaps	15,1	~8,44	~1,79
	Decaps	14,5	~7,94	~1,83
Z1024	KeyGen	33,2	~28,8	~1,15
	Encaps	38,4	~16,21	~2,37
	Decaps	40,7	~17,21	~2,36

Данные отражают ожидаемое время выполнения операций трех этапов инкапсуляции: KeyGen, Encaps и Decaps в модифицированной схеме, а также соответствующий коэффициент ускорения по сравнению с оригинальной реализацией.

Анализ полученных результатов позволяет выявить несколько важных закономерностей. Наиболее существенный выигрыш в производительности достигается для операций инкапсуляции и декапсуляции, где прогнозируемое ускорение составляет от 1,79 до 2,37 раз. Это напрямую связано с высокой вычислительной насыщенностью данных алгоритмов операциями полиномиального умножения, доля которых в общей производительности (времени выполнения) KEM Zemlyanika достигает 66 % для Z512 и 87 % для Z1024. Напротив, процедура генерации ключей демонстрирует скромное ускорение (~1,15 раз), т. к. в меньшей степени зависит от полиномиальной арифметики. Важно отметить ярко выраженную зависимость эффективности оптимизации от размерности модуля k: для набора Z1024 ($k = 4$), где количество операций умножения максимально, достигается наибольший абсолютный и относительный выигрыш, что подтверждает обоснованность предлагаемой в работе модификации.

Проведенная апробация подтверждает не только вычислительные преимущества, но и сохранение криптографической надежности модифицированной схемы KEM Zemlyanika. Увеличение вероятности ошибки расшифрования остается в пределах менее 0,5 % (менее 1 бита в логарифмической шкале), что является статистически незначимым и не требует корректировки параметров шума. При этом использование квазистепенного модуля сравнимой битовой длины не оказывает существенного влияния на сложность известных решеточных атак в модели Core-SVP (Core Shortest Vector Problem – подход к оценке криптографической стойкости криптосистем на основе решеток, основанный на сложности задачи нахождения кратчайшего вектора), т. к. стойкость определяется геометрическими, а не арифметическими свойствами модуля. Таким образом, апробация демонстрирует, что переход на квазистепенной модуль представляет собой сбалансированное решение, обеспечивающее значительный рост производительности критически важных операций KEM Zemlyanika без ущерба для ее фундаментальных криптографических свойств.

Заключение

В результате проведенного исследования показано, что переход схемы KEM Zemlyanika на квазистепенной модуль редукции позволяет эффективно преодолеть фундаментальные архитектурные ограничения оригинальной реализации, обусловленные использованием степенного модуля. Предлагаемое решение сохраняет высокую скорость модульной арифметики, характерную для степенных модулей, и одновременно обеспечивает возможность применения точного и асимптотически оптимального NTT-умножения для полиномов. Это обеспечивает значительное ускорение опера-

ций инкапсуляции и декапсуляции (в диапазоне 1,8–2,6 раз для различных наборов параметров) при минимальном контролируемом снижении границы корректности (около 0,49 %).

Анализ криптографической стойкости показал, что переход на квазистепенной модуль не снижает защиту от известных решеточных атак в модели Core-SVP, т. к. безопасность определяется геометрическими свойствами решетки, а не арифметикой модуля редукции. Неизменность параметров шума и битовой длины модуля позволяет сохранить уровень безопасности, сопоставимый с исходной схемой, а применение NTT упрощает контроль за точностью вычислений и уменьшает структурную сложность алгоритмов, что благоприятно сказывается на потенциальной защите от побочных каналов.

Таким образом, предложенная модификация представляет собой сбалансированное архитектурное решение, которое повышает вычислительную эффективность KEM Zemlyanika, расширяет возможности параметризации и улучшает управляемость ключевых вычислительных операций без ущерба для криптографической стойкости. Результаты исследования создают прочную основу для дальнейшего развития постквантовых схем на базе Module-LWE с оптимизированной архитектурой и высокой практической применимостью.

Список источников

1. Власенко А. В., Евсюков М. В., Путято М. М., Макарян А. С. Исследование реализации механизмов инкапсуляции ключей постквантовых криптографических методов // Прикаспийский журнал: управление и высокие технологии. 2019. № 4 (48). С. 121–127.

2. Малыгина Е. С., Куценко А. В., Новоселов С. А., Колесников Н. С., Бахарев А. О., Хильчук И. С., Шапоренко А. С., Токарева Н. Н. Основные подходы к построению постквантовых криптосистем: описание, сравнительная характеристика // Прикладная дискретная математика. 2023. № 16. С. 58–65. DOI 10.17223/2226308X/16/16.

3. Малыгина Е. С., Куценко А. В., Новосёлов С. А., Колесников Н. С., Бахарев А. О., Хильчук И. С., Шапоренко А. С., Токарева Н. Н. Постквантовые криптосистемы: открытые вопросы и существующие решения криптосистемы на решетках // Дискретный анализ и исследование операций. 2023. Т. 30. № 4 (158). С. 46–90.

4. Zelenetsky A. S., Klyucharev P. G. Zemlyanika – Module-LWE based KEM with the power-of-two modulus, explicit rejection and revisited decapsulation failures // Journal of Computer Virology and Hacking Techniques. 2025. P. 46. DOI 10.1007/s11416-025-00576-y.

5. Avanzi R., Bos J., Ducas L., Klitz E., Lepoint T., Lyubashevsky V., Schanck J. M., Schwabe P., Seiler G., Stehle D. CRYSTALS-Kyber: NIST Post-Quantum Cryptography Project Submission Package Round 3. 2021. P. 31. URL: https://pq-crystals.org/kyber/data/kyber-specification-round3.pdf (дата обращения: 12.12.2025).

6. Bos J., Ducas L., Klitz E., Lepoint T., Lyubashevsky V., Schanck J. M., Schwabe P., Seiler G., Stehle D. CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme // IACR Transactions on Cryptographic Hardware and Embedded Systems. 2018. P. 31.

7. D'Anvers J. P., Guo Q., Johansson T., Nilsson A., Vercauteren F., Verbauwhede I. Decryption failure attacks on IND-CCA secure lattice-based schemes // Public-Key Cryptography – PKC 2019. Lecture Notes in Computer Science. 2019. P. 33.

8. Bodrato M., Zanoni A. Integer and polynomial multiplication: towards optimal Toom-Cook matrices // Proceedings of the International Symprosium on Symbolic and Algebraic Computation. 2007. P. 17–24.

9. Редукция Монтгомери-Баррета и приложение к теоретико-числовому преобразованию Фурье. URL: https://codeforces.com/blog/entry/129600?locale=ru (дата обращения: 12.12.2025).

10. Zelenetsky A. S., Klyucharev P. G. Modular arithmetic optimization in Kyber KEM // Journal of Computer Virology and Hacking Techniques. 2024. P. 857–865.

11. Bos J., Ducas L., Klitz E., Lepoint T., Lyubashevsky V., Schanck J. M., Schwabe P., Seiler G., Stehle D. CRYSTALS-Kyber: A CCA-Secure Module-Lattice-Based KEM // 2018 IEEE European Symposium on Security and Privacy (EuroS&P). 2018. P. 16.

References

1. Vlasenko A. V., Evsyukov M. V., Putyato M. M., Makaryan A. S. Issledovanie realizacii mekhanizmov inkapsulyacii klyuchej postkvantovyh kriptograficheskih metodov [Investigation of the implementation of key encapsulation mechanisms of post-quantum cryptographic methods]. *Prikaspijskij zhurnal: upravlenie i vysokie tekhnologii*, 2019, no. 4 (48), pp. 121-127.

2. Malygina E. S., Kucenko A. V., Novoselov S. A., Kolesnikov N. S., Baharev A. O., Hil'chuk I. S., Shaporenko A. S., Tokareva N. N. Osnovnye podhody k postroeniyu postkvantovyh kriptosistem: opisanie, sravnitel'naya harakteristika [Basic approaches to the construction of post-quantum cryptosystems: description, comparative characteristics]. *Prikladnaya diskretnaya matematika*, 2023, no. 16, pp. 58-65. DOI 10.17223/2226308H/16/16.

3. Malygina E. S., Kucenko A. V., Novosyolov S. A., Kolesnikov N. S., Baharev A. O., Hil'chuk I. S., Shaporenko A. S., Tokareva N. N. Postkvantovye kriptosistemy: otkrytye voprosy i sushchestvuyushchie resheniya kriptosistemy na reshetkah [Post-quantum cryptosystems: open questions and existing solutions Cryptosystems on lattices]. *Diskretnyj analiz i issledovanie operacij*, 2023, vol. 30, no. 4 (158), pp. 46-90.

4. Zelenetsky A. S., Klyucharev P. G. Zemlyanika – Module-LWE based KEM with the power-of-two modulus, explicit re-jection and revisited decapsulation failures. *Journal of Computer Virology and Hacking Techniques*, 2025, p. 46. DOI 10.1007/s11416-025-00576-y.

5. Avanzi R., Bos J., Ducas L., Klitz E., Lepoint T., Lyubashevsky V., Schanck J. M., Schwabe P., Seiler G.,

Stehle D. *CRYSTALS-Kyber: NIST Post-Quantum Cryptography Project Submission Package Round 3*. 2021. P. 31. Available at: https://pq-crystals.org/kyber/data/kyber-specification-round3.pdf (accessed: 12.12.2025).

6. Bos J., Ducas L., Klitz E., Lepoint T., Lyubashevsky V., Schanck J. M., Schwabe P., Seiler G., Stehle D. CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2018, p. 31.

7. D'Anvers J. P., Guo Q., Johansson T., Nilsson A., Vercauteren F., Verbauwhede I. Decryption failure attacks on IND-CCA secure lattice-based schemes. *Public-Key Cryptography – PKC 2019. Lecture Notes in Computer Science*. 2019. P. 33.

8. Bodrato M., Zanoni A. Integer and polynomial multiplication: towards optimal Toom-Cook matrices. *Proceedings of the International Symprosium on Symbolic and Algebraic Computation*. 2007. Pp. 17-24.

9. *Redukciya Montgomeri-Barreta i prilozhenie k teoretiko-chislovomu preobrazovaniyu Fur'e* [Montgomery-Barrett reduction and application to the number-theoretic Fourier transform]. Available at: https://codeforces.com/blog/entry/129600?locale=ru (accessed: 12.12.2025).

10. Zelenetsky A. S., Klyucharev P. G. Modular arithmetic optimization in Kyber KEM. *Journal of Computer Virology and Hacking Techniques*, 2024, pp. 857-865.

11. Bos J., Ducas L., Klitz E., Lepoint T., Lyubashevsky V., Schanck J. M., Schwabe P., Seiler G., Stehle D. CRYSTALS-Kyber: A CCA-Secure Module-Lattice-Based KEM. *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*, 2018, p. 16.

Статья поступила в редакцию 12.01.2026; одобрена после рецензирования 06.02.2026; принята к публикации 16.04.2026
The article was submitted 12.01.2026; approved after reviewing 06.02.2026; accepted for publication 16.04.2026

Информация об авторах / Information about the authors

Надежда Валерьевна Давидюк – кандидат технических наук, доцент; заведующий кафедрой информационной безопасности; Астраханский государственный технический университет; n.davidyuk@astu.ru

Nadezhda V. Davidyuk – Candidate of Technical Sciences, Assistant Professor; Head of the Department of Information Security; Astrakhan State Technical University; n.davidyuk@astu.ru

Феликс Загидинович Эфендиев – магистрант кафедры информационной безопасности; Астраханский государственный технический университет; felixaf1999@mail.ru

Felix Z. Efendiev – Master's Course Student of the Department of Information Security; Astrakhan State Technical University; felixaf1999@mail.ru

Георгий Александрович Попов – доктор технических наук, профессор; профессор кафедры информационной безопасности; Астраханский государственный технический университет; Kaf_ib@astu.ru

Georgy A. Popov – Doctor of Technical Sciences, Professor; Professor of the Department of Information Security; Astrakhan State Technical University; Kaf_ib@astu.ru